UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/038,169 | 01/02/2002 | Dan Boneh | 36321-8009.US01 | 7811 |

22918 7590 04/30/2008
PERKINS COIE LLP
P.O. BOX 2168
MENLO PARK, CA 94026

| EXAMINER | |
|---|---|
| TO, BAOTRAN N | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2135 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 04/30/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/038,169 | BONEH ET AL. | |
| | Examiner | Art Unit | |
| | Baotran N. To | 2135 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *07 February 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-3,5,7-24 and 26-31* is/are pending in the application.

4a) Of the above claim(s) *4, 6 and 25 (Canceled)* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5,7-13,18-24 and 28-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *03/31/08*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

**DETAILED ACTION**

1. This Office action is responsive to the Applicant's Amendment filed 02/07/2008.

Claims 1, 2, 18, 23, 28 and 29 are currently amended.

Claims 14-17 and 26-27 are previously withdrawn.

Claims 4, 6 and 25 are previously canceled.

Claims 1-3, 5, 7-24, 26-31 are pending in the application.

***Response to Arguments***

2. Applicant's arguments filed 02/07/2008 have been fully considered but they are not persuasive.

Applicant argues that Lewis does not disclose "an appliance inserted between the client and the server having a server environment" (Page 11 of Remarks).

Examiner respectfully disagrees with applicant. Lewis explicitly discloses "an appliance inserted between the client and the server having a server environment" which is described in Figure 3, element 2n as (a client), element 180 as (an appliance), and element 300 as (a server).

Applicant further argues that "Lewis does not disclose encrypts the specific sensitive data (Page 11 of Remarks).

Examiner respectfully disagrees. Lewis expressly discloses "all purchase and refund requests will be digitally signed and encrypted for transmission from the hosts 10n to the transaction server 180" (col. 14, lines 26-28).

Applicant further argues that Lewis does not disclose "decrypts the encrypted sensitive data in response to the at least one electronic information query" (Page 12 of Remarks).

Examiner respectfully disagrees. Lewis expressly discloses "After the user fills out the entire field on the purchase screen and selects a submit radio button, the transaction 180 immediately

constructs a new purchase request object base from these field values. After the transaction server 180 receives the purchase request, the purchase request object is deciphered by the transaction server 180 (col. 16, line 59 – col. 17, line 3).

Applicant further argues that Bellwood does not disclose "evaluates the at least one electronic transaction query to specify sensitive data" (Page 13 of Remarks).

Examiner respectfully disagrees. Bellwood expressly discloses "the client sends a secure HTTP request for a service on the original server..., the proxy may decrypt the request, and modify it as needed, and then encrypt the new request and send it to the original server" (col. 6, lines 9-13).

Applicant further argues that " The proxy does not evaluate the request to specify sensitive data because the entire request is presumed to be encrypted before being transmitted to the proxy. In addition, the proxy encrypts the entire request without discretion before sending it to the original server" (Page 13 of Remarks).

Examiner respectfully disagrees. The above argument is not persuasive because it is not related to the scope of the claim limitation.

For at least the above reasons, it is believed that the rejection is maintained.

***Information Disclosure Statement***

3. The information disclosure statement (IDS) submitted on 03/31/2008. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-3, 5, 8-13, 18-24 and 28-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis et al. (U.S. Patent 6,233,565 B1) herein referred to as Lewis in view of Bellwood et al. (U.S. Patent 6,584,567 B1) herein referred to as Bellwood.

Regarding Claims 1 and 28, Lewis discloses a system:

a server (element 4/element 300) having a server environment, wherein, in a first stage, the server and a client (element 2n) are coupled using a protocol to establish at least one secure channel (SSL) (Figure 7, col. 15, lines 42-45, col. 28, lines 50-61 and col. 29, lines 50-66);

an appliance (element 180), wherein in a second stage the appliance is inserted between the client and the server (Figures 2 and 3), wherein the protocol is pre-existing because it was used in the first stage to couple the client and the server (col. 14, lines 26-28, and wherein the appliance:

intercepts at least one electronic transaction query (transaction request) from the at least one client computer (client) via at least one secure channel using the pre-existing protocol (col. 5, lines 30-40 and col. 15, lines 40-45);

encrypts the specified sensitive data only (col. 14, lines 26-28);

transfers, using the pre-existing protocol, the encrypted sensitive data among components of the server environment (col. 14, lines 35-42 and col. 29, lines 27-34), wherein the encrypted sensitive data is stored in one or more components of the server environment (col. 14, lines 55-62);

receives at least one electronic information query for the encrypted sensitive data from at least one third-party system via the at least one secure channel (col. 14, lines 25-29);

obtains the encrypted sensitive data from the server (col. 25, lines 53-60);

decrypts the encrypted sensitive data in response to the at least one electronic information query (col. 16, line 59 – col. 17, line 3);

provides the decrypted sensitive data to the at least one third-party system via the at least one secure coupling (private network connection) (col. 17, lines 1-5).

Lewis does not disclose "evaluates the at least one electronic transaction query to specify sensitive data; wherein the server is incapable of distinguishing between data from the client that does not pass through the appliance and data from the client that was intercepted by the appliance."

However, Bellwood expressly discloses evaluates the at least one electronic transaction query for sensitive data; wherein the server is incapable of distinguishing between data from the client that does not pass through the appliance and data from the client that was intercepted by the appliance" (Abstract, col. 2, lines 19-26 and col. 6, lines 10-17).

Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Bellwood's invention with Lewis to include evaluates the at least one electronic transaction query for sensitive data; wherein the server is incapable of distinguishing between data from the client that does not pass through the appliance and data from the client that was intercepted by the appliance. One of ordinary skill in the art would have been motivated to do so because it would provide the privacy of a secure session between a client and on or more origin servers (Bellwood, col. 1 lines 10-12).

Regarding Claim 2, Lewis discloses a method comprising:

at least one electronic request (transaction request) received from a client (element 2n) over at least one secure channel established (SSL) for sensitive data, using a communication protocol,

between the client and a server (element 4/element 300) having an associated server environment (Figure 7, col. 15, lines 42-45, col. 28, lines 50-61 and col. 29, lines 50-66);

applying at least one cryptographic operation to the sensitive data specified in response to the at least one electronic request, yielding sensitive data in a first form (col. 14, lines 25-30);

transmitting the sensitive data in the first form to the server using the communication protocol (col. 14, lines 35-42 and col. 29, lines 27-34),

wherein the sensitive data in the first form is encrypted (col. 17, lines 51-56).

Lewis does not discloses "evaluating at least one electronic request; yielding sensitive data in a second form, before transfer among components of the server environment; wherein the sensitive data in the second form is decrypted, yielding the sensitive data in the first form, before transfer from the server environment."

However, Bellwood expressly discloses evaluating at least one electronic request ; yielding sensitive data in a second form, before transfer among components of the server environment; wherein the sensitive data in the second form is decrypted, yielding the sensitive data in the first form, before transfer from the server environment (col. 6, lines 10-20).

Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Bellwood's invention with Lewis to include evaluating at least one electronic request; yielding sensitive data in a second form, before transfer among components of the server environment; wherein the sensitive data in the second form is decrypted, yielding the sensitive data in the first form, before transfer from the server environment. One of ordinary skill in the art would have been motivated to do so because it would provide the privacy of a secure session between a client and on or more origin servers (Bellwood, col. 1 lines 10-12).

Regarding Claim 3, Lewis and Bellwood disclose the limitations as discussed in Claim 2 above. Lewis further discloses comprising determining that the at least one electronic request includes sensitive data (col. 14, lines 35-40).

Regarding Claim 5, Lewis and Bellwood disclose the limitations as discussed in Claim 2 above. Lewis further discloses determining that sensitive data in the electronic request includes at least one user password; and applying at least one hash function to the at least one user password (col. 22, lines 58-63).

Regarding Claim 8, Lewis and Bellwood disclose the limitations as discussed in Claim 2 above. Lewis further discloses wherein the at least one electronic request comprises at least one protocol over Secure Socket Layer (col. 15, col. 40-45).

Regarding Claims 9 and 21, Lewis and Bellwood disclose the limitations as discussed in Claim 2 above. Lewis further discloses wherein the sensitive data comprises at least one data item selected from a group including credit card numbers, credit card information, account numbers, account information, birth dates, social security numbers, user information, and user passwords (col. 17, lines 5-15).

Regarding Claim 10, Lewis and Bellwood disclose the limitations as discussed in Claim 2 above. Lewis further discloses executing the at least one cryptographic operation using at least one public key (col. 22, lines 20-25).

Regarding Claims 11 and 22, Lewis and Bellwood disclose the limitations as discussed in Claim 2 above. Lewis further discloses wherein the at least one cryptographic operation includes at least one operation selected from a group including encryption operations, decryption operations, hash operations, keyed hash operations, and keyed hash verification (col. 22, lines 60-65).

Regarding Claim 12, Lewis and Bellwood disclose the limitations as discussed in Claims 2, above. Lewis further discloses wherein encrypting includes performing at least one operation on the sensitive data selected from a group including hashing and keyed hashing when the sensitive data is a password (col. 22, lines 58-64).

Regarding Claim 13, Lewis and Bellwood disclose the limitations as discussed in Claim 2 above. Lewis further discloses wherein the at least one electronic request comprises at least one encoded key identifier (col. 23, lines 25-35).

Regarding Claim 18, Lewis discloses a system, comprising:

at least one client computer (element 2n) coupled to at least one server site (element 4) using a network protocol to establish at least one secure channel over at least one network (SSL) (Figure 7, col. 15, lines 42-45, col. 28, lines 50-61 and col. 29, lines 50-66)

at least one processing device (element 180) coupled among the at least one server site, the at least one client computer and the at least one network for sensitive data (FIG. 2, col. 5, lines 30-40 and col. 15, col. 40-45),

wherein, in operation, the at least one processing device applies at least one cryptographic operation specifically to sensitive data in response to the at least one electronic request (col. 14, lines 25-28),

wherein the sensitive data of the at least one electronic request is encrypted prior to transfer among components of the at least one server site (col. 14, lines 26-28),

wherein encrypted sensitive data of the at least one server site is decrypted prior to transfer among the at least one network (col. 17, lines 1-3).

Lewis does not disclose "evaluates at least one electronic request from the at least one client computer to the at least one server site receive via the at least one network."

However, Bellwood expressly discloses evaluates at least one electronic request from the at least one client computer to the at least one server site receive via the at least one network (col. 6, lines 10-30).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Bellwood's invention with Lewis to include evaluates at least one electronic request from the at least one client computer to the at least one server site receive via the at least one network. One of ordinary skill in the art would have been motivated to do so because it would provide the privacy of a secure session between a client and on or more origin servers (Bellwood, col. 1 lines 10-12).

Regarding Claim 19, Lewis and Bellwood disclose the limitations as discussed in Claim 18 above. Lewis further discloses wherein the at least one processing device determines that the at least one electronic request includes sensitive data by identifying tags indicating that associated data is the sensitive data (col. 6, lines 1-15).

Regarding Claim 20, Lewis and Bellwood disclose the limitations as discussed in Claim 18 above. Lewis further discloses wherein the at least one processing device determines that the at least one electronic request includes sensitive data by identifying tags specified by at least one system administrator that associated data is the sensitive data (col. 6, lines 1-15).

Regarding Claim 23, Lewis discloses a cryptographic appliance, comprising:

at least one processing device (element 180) coupled among at least one server system and at least one network coupling to evaluate at least one received electronic request in a first protocol format (col. 5, lines 30-40 and col. 15, lines 40-45),

wherein the at least one processing device (server) (FIG. 2);

encrypts the sensitive data in the at least one received electronic request (col. 14, lines 26-28).

Lewis explicitly does not disclose "determines whether the at least one received electronic request includes sensitive data."

However, Bellwood expressly discloses determines whether the at least one received electronic request includes sensitive data (col. 6, lines 10-30).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Bellwood's invention with Lewis to include determines whether the at least one received electronic request includes sensitive data. One of ordinary skill in the art would have been motivated to do so because it would provide the privacy of a secure session between a client and on or more origin servers (Bellwood, col. 1 lines 10-12).

Lewis and Bellwood disclose the limitations as discussed in Claim 23 above. Lewis further discloses reforms the electronic request, including the encrypted sensitive data, without deviating from the parameters of the first protocol format (Bellwood, col. 8, lines 45-50); transfers the reformed electronic request, in the first protocol format among at least one component of the at least one server system (Lewis, col. 29, lines 27-34 and Bellwood, col. 6, lines 10-30).

Regarding Claim 24, Lewis and Bellwood disclose the limitations as discussed in Claim 23 above. Lewis further discloses wherein the at least one processing device:

evaluates at least one request for the encrypted sensitive data received via at least one coupling with at least one third-party system (col. 2, lines 30-40);

decrypts the encrypted sensitive data (col. 14, lines 26-28); and

transfers the decrypted sensitive data to the at least one third-party system (col. 17, lines 1-5).

Regarding Claim 29, Lewis a device comprising:

a processor (Figure 2);

a network interface coupled to the processor (Figure 2);

a pattern specification engine coupled to the processor (Figure 2);

a cryptographic engine coupled to the processor (Figure 2);

wherein, in operation, a client and server establish a connection in accordance with a first protocol (SSL) (Figure 7, col. 15, lines 42-45, col. 28, lines 50-61 and col. 29, lines 50-66);

first one or more packets sent from the client to the server including payload formatted in a first protocol are input on the network interface (col. 5, lines 30-40 and col. 15, lines 40-45);

the cryptographic engine applies a cryptographic transformation specifically to the sensitive data (col. 29, lines 27-34);

the processor forms second one or more packets including the cryptographically transformed sensitive data and the non-sensitive data in the first protocol (col. 14, lines 25-28);

the second one or more packets are output on the network interface (col. 29, lines 27-34);

Lewis does not disclose "the pattern specification matching engine enables a user to apply a regular expression to the payload to specify which portion of the payload includes sensitive data to be encrypted and which portion of the payload includes non-sensitive data before the payload reaches the server."

However, Bellwood expressly discloses the pattern specification matching engine enables a user to apply a regular expression to the payload to specify which portion of the payload includes sensitive data to be encrypted and which portion of the payload includes non-sensitive data before the payload reaches the server (col. 6, lines 10-30).

Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Bellwood's invention with Lewis to include the pattern specification matching engine enables a user to apply a regular expression to the payload to specify which portion of the payload includes sensitive data to be encrypted and which portion of the payload includes non-sensitive data before the payload reaches the server. One of ordinary skill in the art would have been motivated to do so because it would provide the privacy of a secure session between a client and on or more origin servers (Bellwood, col. 1 lines 10-12).

Regarding Claim 30, Lewis and Bellwood disclose the limitations as discussed in Claim 29 above. Lewis further discloses a database of cryptographic keys, wherein, in operation, the cryptographic engine uses a key from the database of cryptographic keys to cryptographically transform the sensitive data (col.22, lines 1-50).

Regarding Claim 31, Lewis and Bellwood disclose the limitations as discussed in Claim 29 above. Lewis further discloses wherein the cryptographic transformation includes decryption or encryption (col. 29, lines 26-35).

5. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis and Bellwood as applied to claim 2 above, and further in view of Devine et al. (U.S. Patent 6,598,167 B2) herein referred to as Devine.

Regarding Claim 7, Lewis and Bellwood disclose the limitations as discussed in Claim 2 above.

Lewis and Bellwood explicitly does not disclose "determining the at least one electronic request includes one or more cookies; identify at least one cookie of the one or more cookies that includes sensitive data; applying at least one cryptographic function or checksum to the at least one cookie."

However, Devine teaches "determining the at least one electronic request includes one or more cookies; identify at least one cookie of the one or more cookies that includes sensitive data; applying at least one cryptographic function or checksum to the at least one cookie" (col. 8, lines 45-60).

Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate Devine's invention with Lewis and Bellwood to have included the cookie with the motivation being to allow adding an additional level of security (col. 8 lines 55-60).

***Conclusion***

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the

mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Baotran N. To whose telephone number is (571)272-8156. The examiner can normally be reached on Monday-Friday from 8:00 to 4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/B. N. T./
Examiner, Art Unit 2135
04/25/2008

/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2135